

监控EIGRP在连结7000上的邻接变化的SNMP陷阱

目录

[概述](#)

[示例](#)

概述

连结只支持EIGRP-MIB的两个陷阱，cEigrpAuthFailureEvent和cEigrpRouteStuckInActive，但是up/down的EIGRP邻居的没有SNMP陷阱(cEigrpNbrDownEvent)。

形成SNMP陷阱的一可行的应急方案监控EIGRP邻接更改是配置-一个邻居的和-一个下来邻居的-被触发的两份EEM脚本基于Syslog模式。

示例

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

您能由飘荡然后测试第3层接口(您可以创建测验SVI验证至于不打乱连接)：

```
event manager applet EIGRP_TRAP_nbr_dwn
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*down"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Down"
event manager applet EIGRP_TRAP_nbr_up
  event syslog pattern "EIGRP-5-NBRCHANGE_DUAL.*up"
  action 1.1 snmp-trap strdata "EIGRP Neighbor Up"
```

确认连结通过检查您的SNMP监控工具发送这些正确地-输出可能根据使用的工具轻微有所不同：



The screenshot shows a network device console output for an SNMP trap. The text includes: "No Trap Parser defined for received trap: TrapOid: .1.3.6.1.4.1.9.10.134.0.2", "Variable Bindings: sysUpTime.0: 305 days, 23 hours, 40 minutes, 20 seconds.", "snmpTrapOID.0: .1.3.6.1.4.1.9.10.134.0.2, .1.3.6.1.4.1.9.10.134.1.2.3.1.2.1: 8449, .1.3.6.1.4.1.9.10.134.1.2.3.1.6.1: .1.3.6.1.4.1.9.10.134.1.2.3.1.7.1: EIGRP_TRAP, .1.3.6.1.4.1.9.10.134.1.2.3.1.9.1: 0, .1.3.6.1.4.1.9.10.134.1.2.3.1.10.1: 0, .1.3.6.1.4.1.9.10.134.1.2.3.1.11.1: EIGRP adjacency change." The console also shows "Info Events" and "Info" messages, and a timestamp "14 Jul 2017 10:07:08 AM EDT".

您可以通过Wireshark捕获也查看这些SNMP陷阱：

注意：根据Wireshark版本，字符串不会在人类易读的文本，然而可以通过“snmp.value.octets被过滤包含“EIGRP””

Capturing from 3 interfaces [Wireshark 1.10.3-Spirent-2 (SVN Rev Unkn)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: snmp.value.octets contains "EIGRP" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
14	10.5091510	10.122.140.96	172.18.121.3	SNMP	278	snmpv2-trap 1.3.6.1.2.1.1.3.0 1.

Frame 14: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits) on interface 1

- Ethernet II, Src: Cisco_66:8a:c4 (00:13:80:66:8a:c4), Dst: Vmware_be:56:b8 (00:50:56:be:56:b8)
- Internet Protocol Version 4, Src: 10.122.140.96 (10.122.140.96), Dst: 172.18.121.3 (172.18.121.3)
- User Datagram Protocol, Src Port: 37782 (37782), Dst Port: snmptrap (162)
- Simple Network Management Protocol
 - version: v2c (1)
 - community: public
 - data: snmpv2-trap (7)
 - snmpv2-trap
 - request-id: 121
 - error-status: noError (0)
 - error-index: 0
 - variable-bindings: 8 items
 - 1.3.6.1.2.1.1.3.0: 52260863
 - 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.9.10.134.0.2 (iso.3.6.1.4.1.9.10.134.0.2)
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1: 8449
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1: <MISSING>
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.7.1: 45494752505f54455354
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1:
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1:
 - 1.3.6.1.4.1.9.10.134.1.2.3.1.11.1: 45494752502061646a6163656e6379206368616e6765

您能也验证连结发送这些在触发与Ethanalyzer的EEM -示例：

```
N7K-A-Admin# ethanalyzer local interface mgmt display-filter snmp limit-c 0
```

```
Capturing on mgmt0
```

```
2017-07-12 15:43:37.431067 10.122.140.96 -> 172.18.121.3 SNMP 278 snmpv2-trap 1.3.6.1.2.1.1.3.0
1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.10.134.1.2.3.1.2.1 1.3.6.1.4.1.9.10.134.1.2.3.1.6.1
1.3.6.1.4.1.
9.10.134.1.2.3.1.7.1 1.3.6.1.4.1.9.10.134.1.2.3.1.9.1 1.3.6.1.4.1.9.10.134.1.2.3.1.10.1
1.3.6.1.4.1.9.10.134.1.2.3.1.11.1
```

注意：前NX-OS 7.x不给出我们配置“反之将允许您监控整个记录日志日志为EIGRP消息然后过滤的snmp-server enable traps Syslog的”选项。此功能在最新版本被添加了，7.x和以后。